Amendments to and Listing of the Claims:

Please cancel claims 2, 5, and 7. Please amend claims 1, 3, 4, 6, 8, 9, and 12 as indicated below, wherein double bracketing and strikethrough each indicate deletion and underlining indicates addition. This listing of claims will replace all prior versions and listings of claims in the application.

1. (Currently amended) A method for determining the Nth state of an n-stage linear feedback shift register (LFSR) providing a result useful in applications including password generation, convergent signature analysis, and encryption, comprising steps of:

building a look-up table of n-bit states for latch positions of said linear feedback shift register;

obtaining a modulo remainder of said Nth state; and

generating directly from said modulo remainder and said n-bit states said Nth state[[.]] and, if in standard form, further comprising steps of:

converting said LFSR to modular form;

modulo (2^n-1) dividing a desired cycle count N to derive a remainder value N";

building said look-up table to include x, y, and z values, where

x=LFSR latch position (0, 1, . . . , n-1);

$y=2^i$ for i=0, n-1 (for i=0, 1, 2, 3, . . . , n-1), giving values (0, 1, 2, 4, 8, . . . , 2^{n-1}); and

z=n-bit state of said LFSR for (x, y);

first determining all cycle rows Ci needed to binary add to said remainder value N";

for each said bit position y in a first said cycle row Ci, second determining said n-bit state z;

for each bit set in each said n-bit state z, third determining for a next cycle row Ci said n-bit state z; and

exclusive ORing all said n-bit states to determine said Nth state.

2. (Cancelled)

3. (Currently amended) The method of claim [[2]] 1, said third determining step comprising:

identifying for each bit set in said remainder value N" a corresponding cycle row y;

for a first identified cycle row in N", determining from said look-up table a corresponding n-bit state $S_{\text{first cycle row}}$; and

for each bit set in said n-bit state $S_{\text{first cycle row}}$, next determining from said look-up table a next corresponding n-bit state $S_{\text{next cycle row}}$;

repeating said next determining step until all final states $S_{\text{final cycle row}}$ are reached for said bit set in said n-bit state $S_{\text{first cycle row}}$; [[and]]

exclusive ORing all said final states for said bit set in said n-bit state; and

repeating said determining steps until processing all bits set in said LFSR.

4. (Currently amended) A ~~program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine~~ computer program product comprising a computer useable medium having a computer readable program, wherein the computer readable program when executed on a computer causes the computer to perform method steps for determining the Nth state of an n-stage linear feedback shift register (LFSR), providing a result useful in applications including password generation, convergent signature analysis, and encryption, said method comprising:

building a look-up table of n-bit states for latch positions of said linear feedback shift register;

obtaining a modulo remainder of said Nth state; and

generating directly from said modulo remainder and said n-bit states said Nth state[[.]] and, if in standard form, further comprising steps of:

converting said LFSR to modular form;

modulo (2^n-1) dividing a desired cycle count N to derive a remainder value N";

building said look-up table to include x, y, and z values, where

x=LFSR latch position (0, 1, . . . , n-1);

$y=2^i$ for i=0, n-1 (for i=0, 1, 2, 3, . . . , n-1), giving values (0, 1, 2, 4, 8, . . . , 2^{n-1}); and

z=n-bit state of said LFSR for (x, y);

identifying for each bit set in said remainder value N" a corresponding cycle row y;

for a first identified cycle row in N", determining from said look-up table a corresponding n-bit state $S_{\text{first cycle row}}$;

for each bit set in said n-bit state $S_{\text{first cycle row}}$, next determining from said look-up table a next corresponding n-bit state $S_{\text{next cycle row}}$;

repeating said next determining step until all final states $S_{\text{final cycle row}}$ are reached for said bit set in said n-bit state $S_{\text{first cycle row}}$;

exclusive ORing all said final states for said bit set in said n-bit state;

repeating said determining steps until processing all bits set in said LFSR; and

exclusive ORing all said final states for all said bits set in said LFSR to determine said Nth state of said LFSR.

5. (Cancelled)

6. (Currently amended) A system for determining the Nth state of an n-stage linear feedback shift register (LFSR), providing a result useful in applications including password generation, convergent signature analysis, and encryption, comprising:

means for building a look-up table of n-bit states for latch positions of said linear feedback shift register;

means for obtaining a modulo remainder of said Nth state; [[and]]

means for generating said Nth state directly from said modulo remainder and said n-bit states[[.]];

means for converting said LFSR to modular form if in standard form;

means for modulo (2^n-1) dividing a desired cycle count N to derive a remainder value N";

means for building said look-up table to include x, y, and z values, where

x=LFSR latch position (0, 1, . . . , n-1);

$y=2^i$ for i=0, n-1 (for i=0, 1, 2, 3, . . . , n-1), giving values (0, 1, 2, 4, 8, . . . , 2^{n-1}); and

z=n-bit state of said LFSR for (x, y);

first means for determining all cycle rows Ci needed to binary add to said remainder value N";

second means for determining said n-bit state z for each said bit position y in a first said cycle row Ci;

third means for determining for a next cycle row Ci said n-bit state z for each bit set in each said n-bit state z; and

means for exclusive ORing all said n-bit states to determine said Nth state.

7. (Cancelled)

8. (Currently amended) The system of claim [[7]] 6, said third means further comprising:

means for identifying for each bit set in said remainder value N" a corresponding cycle row y;

means for determining from said look-up table a corresponding n-bit state $S_{\text{first cycle row}}$ for a first identified cycle row in N";

means for processing each bit set in said n-bit state $S_{\text{first cycle row}}$, to determine from said look-up table a next corresponding n-bit state $S_{\text{next cycle row}}$;

fourth means for executing said means for processing until all final states $S_{\text{final cycle row}}$ are reached for said bit set in said n-bit state $S_{\text{first cycle row}}$; and then for exclusive ORing all said final states for said bit set in said n-bit state; and

fifth means for repeating execution of said fourth means for all bits set in said LFSR.

9. (Currently amended) The ~~program storage device~~ computer program product of claim [[5]] 4, said method further comprising responsive to said Nth state, selectively executing at least

one of password generation, convergent signature analysis, secure credit card processing, system security integration, and encryption encoding and decoding.

10. (Original) The system of claim 8, further comprising means responsive to said Nth state for selectively executing at least one of password generation, convergent signature analysis, secure credit card processing, system security integration, and encryption encoding and decoding.

11. (Original) The method of claim 1, further comprising responsive to said Nth state, selectively executing at least one of password generation, convergent signature analysis, secure credit card processing, system security integration, and encryption encoding and decoding.

12. (Currently amended) The ~~program storage device~~ computer program product of claim [[5]] 4, said method further comprising selectively compressing data and generating signatures responsive to said Nth state.